UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/066,232	01/31/2002	Massimiliano Antonio Poletto	12221-010001	2754

26161 7590 08/04/2006

FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
PERUNGAVOOR, VENKATANARAY	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 08/04/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/066,232	POLETTO ET AL.	
	Examiner	Art Unit	
	Venkat Perungavoor	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 May 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

In view of the Appeal Brief filed on 5/26/2006, PROSECUTION IS HEREBY REOPENED. Details set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

1. Applicant's arguments with respect to claims 1-40 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 7, 9-14, 19-23, 26 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S Patent 6,769, 066 B1 to Botros et al.(hereinafter Botros).

4. Regarding Claim 7, 21, Botros discloses the producing of histogram of received network traffic based on parameters see Col 10 Ln 40-53 & Fig. 14 item 1402; characterization of attack based on comparison of historical histogram of data for parameter see Col 8 Ln 28-39 & Fig. 14 item 1404.

5. Regarding Claim 9 and 10, Botros discloses the varying of time to get an accurate historical data see Col 7 Ln 24-57.

6. Regarding Claim 11, 23, Botros discloses the normalizing of the histograms and computing the difference to significant outliner of suspicious traffic see Col 9 Ln 24-50.

7. Regarding Claim 13, Botros discloses the feature vector containing an list of anomalous behavior see Col 8 Ln 46-67.

8. Regarding Claim 12 and 14, 22, Botros discloses the correlation process that correlates the parameters and indicates the types of attacks see Col 13 Ln 24-41.

9. Regarding Claim 19 and 20, 26, Botros discloses the data collector see Fig. 3 item 202 and gateway see item 200.

10. Regarding Claim 21, Botros discloses the computing device see Fig. 2 item 104, producing of histogram of received network traffic based on parameters see Col 10 Ln 40-53 & Fig. 14 item 1402; characterization of attack based on comparison of historical histogram of data for parameter see Col 8 Ln 28-39 & Fig. 14 item 1404.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 1-6, 8, 15-18, 24-25, 27, 30-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S Patent 6,769, 066 B1 to Botros et al.(hereinafter

Botros) in view of U.S. Patent 2002/0107960 A1 to Wetherall et al.(hereinafter Wetherhall).

13. Regarding Claim 1, 28, Botros discloses the monitoring of device for attacks where detecting process to determine if the parameter of network traffic exceed normal value see Col 10 Ln 40-53 & Col 9 Ln 1-23; a process to build histogram for the parameter see Fig. 9 item 904 & Fig. 10. But does not disclose a filtering of network packets based on the characterization process using histogram for parameter to compute significant outliers in a parameter and classify the attack. However, Wetherall discloses the filtering processes based on the characterization process using histogram for parameter to compute significant outliers in a parameter and classify the attack see Fig. 2 item 206, 208, 210, 212.It would be obvious to one having ordinary skill in the art at the time of the invention to include the filtering processes based on the characterization process using histogram in the invention of Botros in order to route out the undesirable packets as taught in Wetherall see Par. 0041.

14. Regarding Claim 2, Botros discloses the vector having bad and good values see Col 9 Ln 51-Col 10 Ln 3.

15. Regarding Claim 3, Botros discloses the correlation process that correlates the parameters and indicates the types of attacks see Col 13 Ln 24-41.

16. Regarding Claim 4, Botros discloses the correlation process being used for reduce false positives see Col 12 Ln 59-Col 13 Ln 3.

17. Regarding Claim 5 and 6, 29, Botros does not discloses the aggregate filtering. However, Wetherall discloses the aggregate filtering see Par. 0041(blanket filtering) and source IP address see Fig. 2 item 208 & 212. For motivation to combine see above Claim 1.

18. Regarding Claim 8, 30-31, Botros discloses the comparison of historical data for ranges see Col 10 Ln 40-53, but does not disclose the filtering process. However, Wetherall discloses the filtering processes based on the characterization process using histogram see Fig. 2 item 206, 208, 210, 212.It would be obvious to one having ordinary skill in the art at the time of the invention to include the filtering processes based on the characterization process using histogram in the invention of Botros in order to route out the undesirable packets as taught in Wetherall see Par. 0041.

19. Regarding Claim 15-18, 24, 27, 38-40, Botros does not discloses the producing of a vector that is constant and constructing a vector for packets to test whether to forward for drop packets from source address. However, Wetherall discloses the producing of a vector that is constant and constructing a vector for packets to

test whether to forward for drop see Par. 0056. It would be obvious to one having ordinary skill in the art at the time of the invention to include the filtering processes based on the characterization process using histogram in the invention of Botros in order to route out the undesirable packets as taught in Wetherall see Par. 0041.

20. Regarding Claim 25, Botros does not disclose the dynamically installing of filters on nearby routers. However, Wetherall discloses the installing of filters on routers see Fig. 1 item 106d & Fig. 2 item 210.

21. Regarding Claim 32, Botros discloses the monitoring of device for attacks where detecting process to determine if the parameter of network traffic exceed normal value see Col 10 Ln 40-53 & Col 9 Ln 1-23 through a gateway see Fig. 2 item 104; a process to build histogram for the parameter see Fig. 9 item 904 & Fig. 10 and comparing it with a historical histogram for a parameter see Col 8 Ln 28-39 & Fig. 14 item 1404. But does not disclose a filtering of network packets based on the characterization process using histogram. Botros further discloses the comparison of historical data for ranges see Col 10 Ln 40-53, but does not disclose the filtering process. However, Wetherall discloses the filtering processes based on the characterization process using histogram see Fig. 2 item 206, 208, 210, 212.It would be obvious to one having ordinary skill in the art at the time of the invention to include the filtering processes based on the

characterization process using histogram in the invention of Botros in order to route out the undesirable packets as taught in Wetherall see Par. 0041.

22. Regarding Claim 33-36, Botros discloses the communicating of statisitics to data center over an secure networks see Fig. 3.

23. Regarding Claim 37, Botros discloses the monitoring of device for attacks where detecting process to determine if the parameter of network traffic exceed normal value see Col 10 Ln 40-53 & Col 9 Ln 1-23; a process to build histogram for the parameter see Fig. 9 item 904 & Fig. 10. But does not discloses the filtering out traffic deemed part of attack by producing/retrieving of a vector that is constant/initialized and constructing a vector for packets to test whether to forward for drop packets from source address based on parameter correlations. However, Wetherall discloses the filtering out traffic deemed part of attack by producing of a vector that is constant/initialized to zero and constructing a vector for packets to test/index whether to forward for drop see Par. 0056. It would be obvious to one having ordinary skill in the art at the time of the invention to include the filtering processes based on the characterization process using histogram in the invention of Botros in order to route out the undesirable packets as taught in Wetherall see Par. 0041.

Conclusion

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Venkat Perungavoor whose telephone number is 571-272-7213. The examiner can normally be reached on 8-4:30. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

25. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Venkat Perungavoor
Examiner
Art Unit 2132

VP
7/28/2006

CHRISTOPHER REVAI
PRIMARY EXAMINER
8/2/06